BSIT 5th

Section A & B

Lecture 03

Local Security Policy

Kashif Ali

Topics to be cover

ACCOUNT LOCKOUT POLICY

PASSWORD POLICY

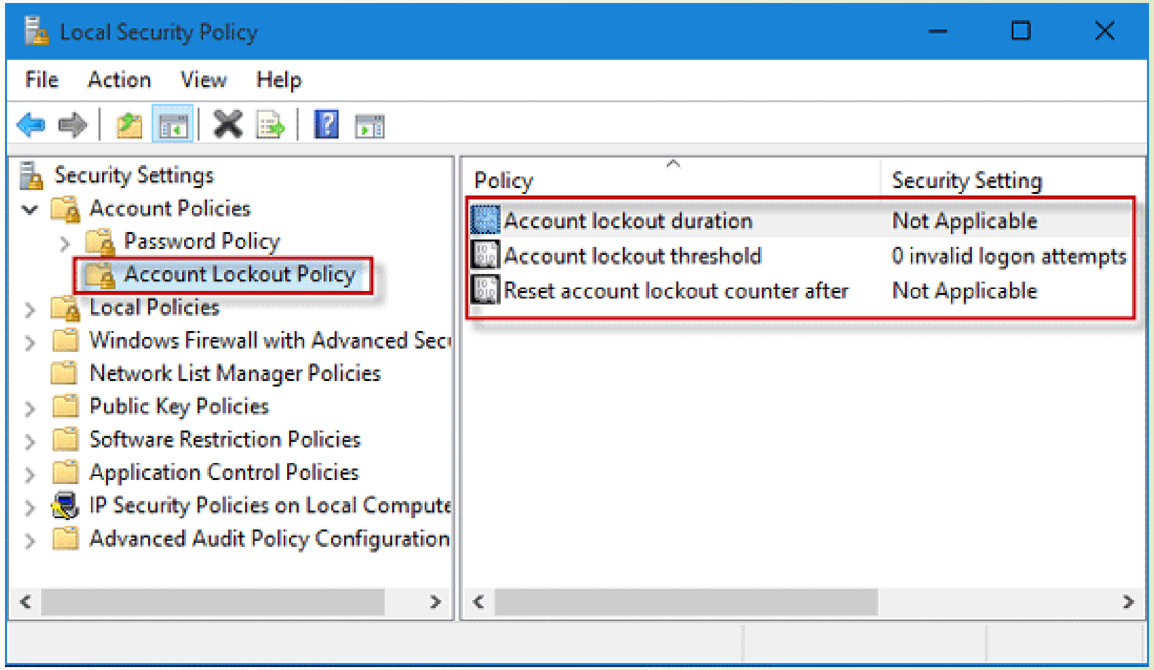
AUDIT POLICY

USER RIGHTS ASSIGNMENTS

SECURITY OPTIONS

Account Lockout Policy

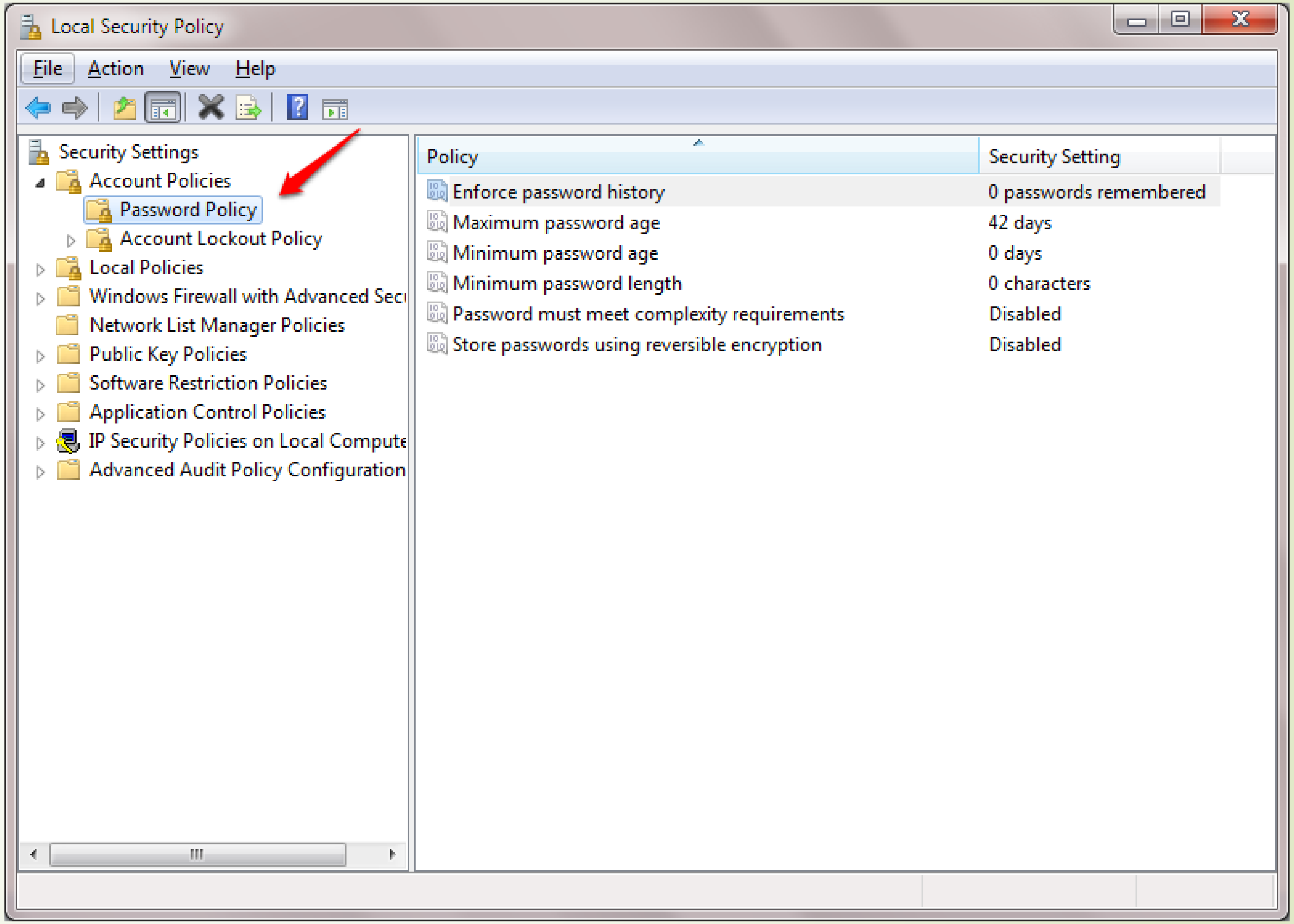
- The Account lockout duration policy setting determines the number of minutes that a locked-out account remains locked out before automatically becoming unlocked.
- The available range is from 1 through 99,999 minutes.
- A value of 0 specifies that the account will be locked out until an administrator explicitly unlocks it.


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Account lockout duration	Not Applicable
Account lockout threshold	0 invalid logon attempts
Reset account lockout counter after	Not Applicable

Password Policy

- Enforce password history
- Maximum password age
- Minimum password age
- Minimum password length
- Password must meet complexity requirements
- Store passwords using reversible encryption


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Enforce password history	0 passwords remembered
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

Enforce Password History

- This allows the user to define the number of unique passwords allowed per user before reusing the old password.
- For example, if the value is set to 5, the user can reuse the first password only after 5 unique password changes.
- By default, the value is not configured.
- The allowed value ranges from 0 to 24.

Maximum Password Age

- Allows the user to set the password duration (in days) after which the user is forced to change the password.
- For example, if the value is set to 30, the user will be prompted to change the password on the thirty-first day.
- By default, the value is not configured.
- The allowed value ranges from 0 to 999.
- If the value is set to 0, that means the password will never expire.

Minimum Password Age

- Allows the user to set the duration (in days) that a password must be used before the user changes it.
- For example, if the value is set to 5, the user can only change the password after 5 days.
- By default, the value is not configured.
- The allowed value ranges from 1 to 998.
- If the value is set to 0, that means the password can be changed immediately.

Minimum Password Length

- Allows the user to set the minimum length of the password.
- For example, if the value is set to 8, the minimum length of the password would be 8 characters and no less than that.
- By default, the value is not configured.
- The allowed value ranges from 1 to 14.
- If the value is set to 0, that means the password is not required.

Password Must Complexity Requirements

If this policy is enabled, passwords must meet the following minimum requirements:

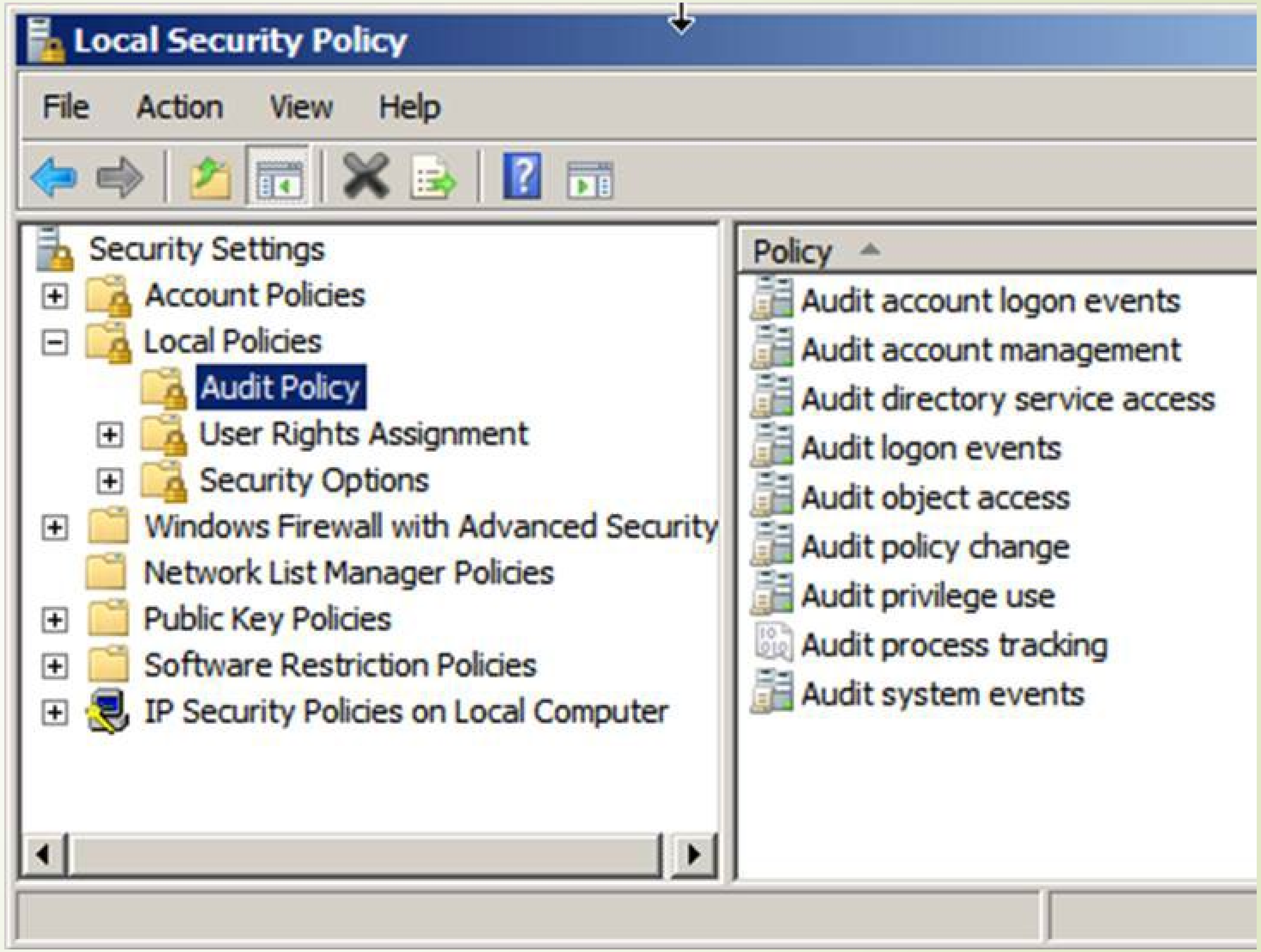
- Not contain the user's account name or parts of the user's full name that exceed two consecutive characters.
- Be at least six characters in length.
- Contain characters from three of the following four categories:
  - English uppercase characters (A through Z)
  - English lowercase characters (a through z)
  - Base 10 digits (0 through 9)
  - Non-alphabetic characters (for example, !, $, #, %)
- Complexity requirements are enforced when passwords are changed or created.
- By default, it is set to disable.

Store Passwords Using Reversible Encryption

- This allows storing encrypted passwords in a way that it can be decrypted.
- This is an unsafe setting and must be disabled.

Audit Policy

- The security audit policy settings under Security Settings\Local Policies\Audit Policy provide broad security audit capabilities for client devices and servers that can't use advanced security audit policy settings.

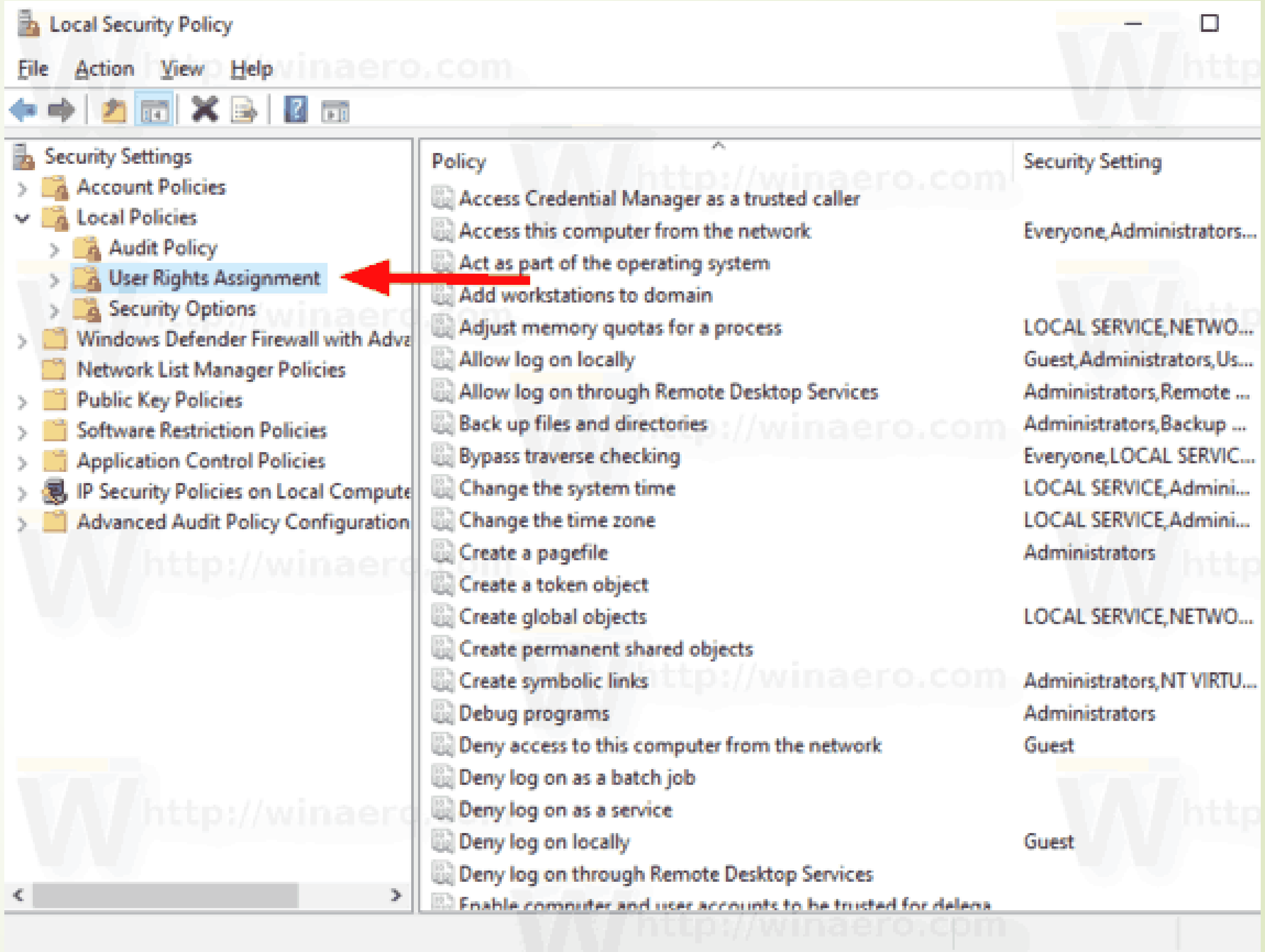


- Security Settings
  - Account Policies
  - Local Policies
    - Audit Policy
    - User Rights Assignment
    - Security Options
  - Windows Firewall with Advanced Security
  - Network List Manager Policies
  - Public Key Policies
  - Software Restriction Policies
  - IP Security Policies on Local Computer

Audit account logon events
Audit account management
Audit directory service access
Audit logon events
Audit object access
Audit policy change
Audit privilege use
Audit process tracking
Audit system events

User Rights Assignment

- User rights are applied at the local computer level, and they allow users to perform tasks on a computer or in a domain.
- User rights include logon rights and permissions.
- Logon rights control who is authorized to log on to a computer and how they can log on.

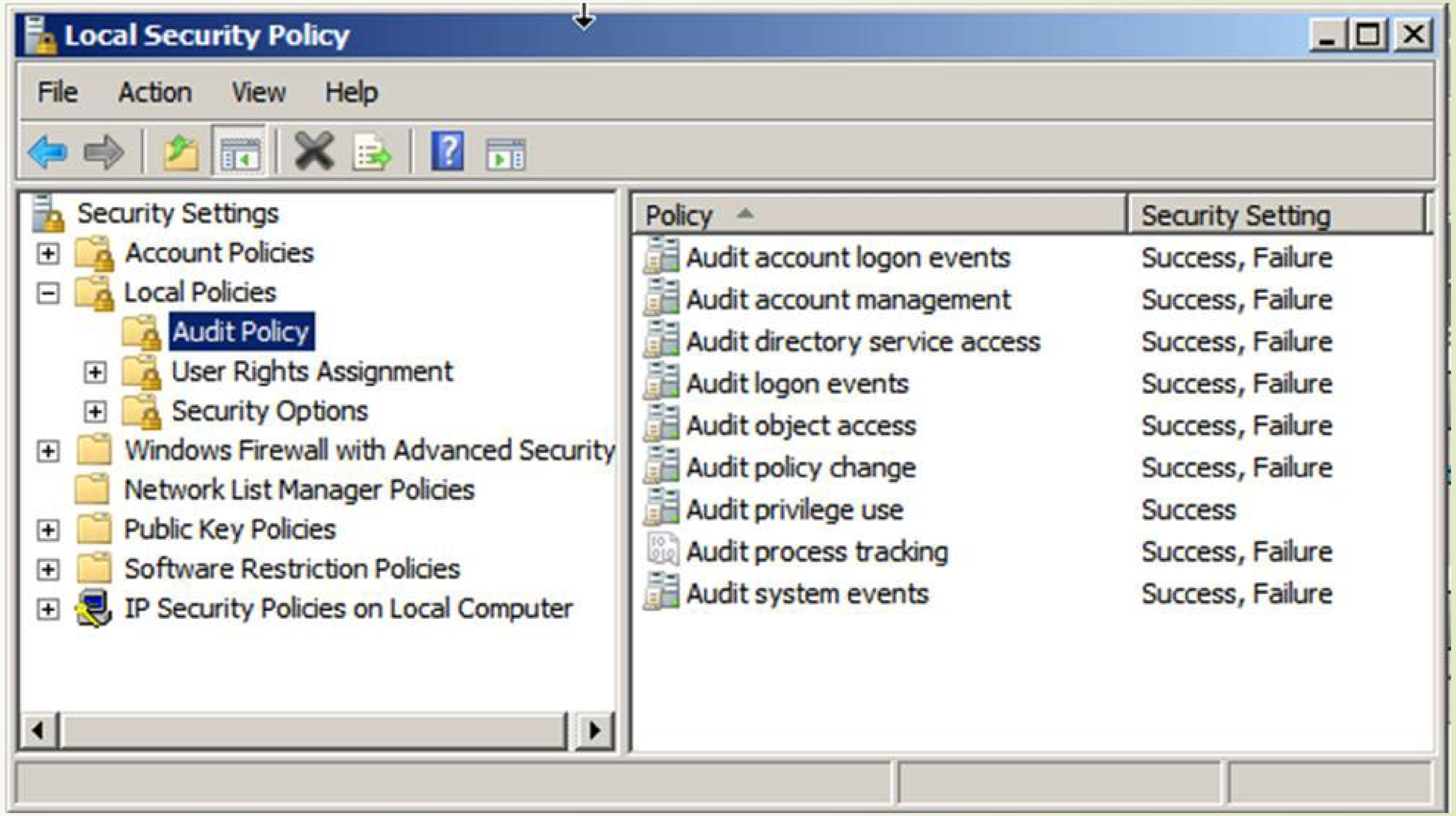


Security Settings
- Account Policies
- Local Policies
  - Audit Policy
  - User Rights Assignment
  - Security Options
- Windows Defender Firewall with Adva
- Network List Manager Policies
- Public Key Policies
- Software Restriction Policies
- Application Control Policies
- IP Security Policies on Local Compute
- Advanced Audit Policy Configuration

Policy	Security Setting
Access Credential Manager as a trusted caller	
Access this computer from the network	Everyone,Administrators...
Act as part of the operating system	
Add workstations to domain	
Adjust memory quotas for a process	LOCAL SERVICE,NETWO...
Allow log on locally	Guest,Administrators,Us...
Allow log on through Remote Desktop Services	Administrators,Remote ...
Back up files and directories	Administrators,Backup ...
Bypass traverse checking	Everyone,LOCAL SERVIC...
Change the system time	LOCAL SERVICE,Admini...
Change the time zone	LOCAL SERVICE,Admini...
Create a pagefile	Administrators
Create a token object	
Create global objects	LOCAL SERVICE,NETWO...
Create permanent shared objects	
Create symbolic links	Administrators,NT VIRTU...
Debug programs	Administrators
Deny access to this computer from the network	Guest
Deny log on as a batch job	
Deny log on as a service	
Deny log on locally	Guest
Deny log on through Remote Desktop Services	
Enable computer and user accounts to be trusted for delega	

Security Options

- Security policy settings are rules that administrators configure on a computer or multiple devices for protecting resources on a device or network.



Policy	Security Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Success, Failure
Audit logon events	Success, Failure
Audit object access	Success, Failure
Audit policy change	Success, Failure
Audit privilege use	Success
Audit process tracking	Success, Failure
Audit system events	Success, Failure

Videos to cover these topics

- https://www.youtube.com/watch?v=U7o9WwcgAu0&list=PLyxg8agb6OW-nXvwHw0kTG22jmSsOfYS1&index=5&ab_channel=KashifBuneriITTrainer

- https://www.youtube.com/watch?v=nCg5v5cKPIg&list=PLyxg8agb6OW-nXvwHw0kTG22jmSsOfYS1&index=6&ab_channel=KashifBuneriITTrainer

kashif.nth@aup.edu.pk

Kashif Ali